IN THE UNITED STATES PATENT & TRADEMARK OFFICE

In re Application of:

Charles C. Brackett	:	Group Art Unit: 2134
Serial No.: 09/667,742	:	Examiner: Heneghan, M.E.

Filed: September 22, 2000

Title: ULTRASOUND IMAGING SYSTEM HAVING VIRUS PROTECTION

Hon. Commissioner for Patents
Alexandria, VA 22313

PRE-APPEAL BRIEF REQUEST FOR REVIEW

In accordance with the OG Notice of July 12, 2005, the Applicant hereby requests review of the Final Rejection mailed on July 20, 2006 in the above-referenced patent application. A Notice of Appeal is being filed concurrently herewith.

In the Final Rejection, claims 1, 4, 8, 9, 11-13, 30-32, and 34-36 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Hiyama (US 6,269,379) in view of McGee (US 6,694,434) and further in view of Lang (US 5,191,611) and Hile (US 5,319,776). Applicant respectfully submits that this rejection is erroneous for the following reasons.

Independent claims 1 and 30 each recite "means for decrypting said encrypted data in said registry file and means for searching said decrypted data for an entry matching the identifier received from said operating system identifying a starting process of said application program to be executed by said operating system."

The Final Rejection cites McGee as teaching registry information that is digitally signed using a private key and

then authenticated (i.e., decrypted) using a public key. However, this feature in McGee is different than Applicant's claimed registry. Applicant's invention includes "a registry file containing encrypted data representing a list of all processes that are approved by the system manufacturer or service provider to run on the imaging system". This registry does not contain encrypted data that is specific to a particular user, but rather contains encrypted data for processes "approved by the system manufacturer or service provider" regardless of who the user is. In other words, all that matters is whether the process is approved, not whether the user of the process is approved. If, as proposed by McGee, the system were to be capable of allowing a user to digitally sign the application registration data using a private signing key, the system would then need to decrypt that data using "the user's public signing key" (see McGee, col. 5, lines 10-12). That "user's" public signing key is specific to the user. Public keys are often stored on public key servers. Each user would have his own public signing key stored in the public key server or registry, if you will. This is clearly different from Applicant's invention, wherein the process to be executed is compared to data obtained by decrypting encrypted data stored in a registry, that encrypted data representing approved processes. Unlike McGee, Applicant's invention does not require the use of encrypted data that identifies the user. Instead the invention authenticates the requested process to be executed using encrypted data that identifies approved processes.

Furthermore, independent claims 1 and 30 each recite that the host computer is programmed to decrypt the encrypted data

in the registry and then search that decrypted data for an entry matching an identifier received from the operating system identifying a starting process of an application program to be executed by the operating system. The McGee patent does not disclose this step, but rather discloses that the computing unit "generates a hash value of a requesting application and evaluates whether the generated hash value matches the centralized registration list" (see McGee, col. 5, lines 17-20). There is no disclosure that the entries in the centralized registration list are decrypted. Furthermore, the digital signature of McGee is an encryption of a hash value derived from a list of hash values generated from the executable files. Conversely, the decryption of that digital signature will be the hash value derived from the list (i.e., multiplicity) of hash values and is not the hash value of any particular executable file. McGee teaches that the execution of files is monitored by comparing the hash values stored in the registry list to the hash value generated from the file to be executed (see McGee, col. 4, lines 25-27). If there is a match, the application is granted execution privileges (see McGee, col. 5, lines 6-7).

More specifically, McGee uses hash values generated using "one-way hash functions", as stated at col. 7, line 28 and col. 8, line 53. A hash function H is a transformation that takes a variable-size input m and returns a fixed-size string, which is called the hash value h (that is $h = H(m)$. One basic requirement of a cryptographic hash function is that it be "one-way". A hash function is said to be "one-way" if it is hard to invert, meaning that given a hash value h, it is

computationally unfeasible to find some input x such that $H(x) = h$. In other words, the one-way hash values disclosed by McGee are not decrypted and could not be decrypted, which is largely due to the fact that the hash values are generated by transforming a large domain into a small range, resulting in lost data that cannot be recovered by inverting the hash function.

Nor does the Lang patent disclose the key features that are missing from McGee. In particular, Lang does not disclose the use of a registry containing encrypted data representing processes approved for execution on a computer. Instead, Lang discloses that a user can access encrypted directories of files by inputting an encrypted security identification code that identifies the user personally. The encrypted directory is then decrypted and then re-encrypted using the user's personal security key. Lang neither discloses nor suggests decrypting a registry of encrypted data representing approved processes and then comparing the decrypted data with the process requested by the user to find a match.

Accordingly, Applicant respectfully submits that neither McGee nor Lang discloses or suggests the monitoring means recited in claims 1 and 30. The Examiner does not assert that Hiyama or Hile disclose that feature either.

Secondly, a *prima facie* case of obviousness has not been shown because there is no motivation or suggestion to import the teachings of McGee into the image filing system of Hiyama, let alone into an ultrasound imaging system. The Examiner cites to a passage in Hiyama (see col. 8, lines 66 and 67)

that teaches the use of a password to prevent unauthorized copying of any file during running of the operating system 82, thereby preventing the "invasion of [a] computer virus into a running application or other program". Since Hiyama has already solved the problem of preventing infection of his image filing system with a computer virus, there would be no need to incorporate the registration system of McGee to solve the same problem.

Accordingly, Applicant respectfully submits that claims 1 and 30 are not obvious in view of Hiyama, McGee, Lang and Hile.

The obviousness rejections set forth in ¶¶ 4 and 5 of the Final Rejection are based on the aforementioned combination of prior art as applied to claim 1 and/or 30 in combination with a fifth reference (namely, Yamamoto or Kisor). These rejections suffer from the same infirmities as those noted above vis-à-vis the Hiyama/McGee/Lang/Hile combination.

In view of the foregoing, the Applicant respectfully submits that the Final Rejection should be overturned.

Respectfully submitted,

October 16, 2006
Date

Dennis M. Flaherty
Reg. No. 31,159

CERTIFICATE OF MAILING

The undersigned hereby certifies that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date set forth below.

October 16, 2006
Date

Dennis M. Flaherty